UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/921,231	07/31/2001	Brian J. Matt	NA01-00101	6007

28875 7590 09/20/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/921,231	MATT, BRIAN J.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-18 and 20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-18 and 20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A Request for Continued Examination with amendment was received on 13 July 2005. Claims 1, 3, 17, 18, and 20 have been amended. Claims 2, 19, and 21 have been canceled. No new claims have been added. Claims 1, 3-18, and 20 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 13 July 2005 have been fully considered but they are not persuasive.

3. All claims were rejected under 35 U.S.C. 112, first and second paragraphs. Regarding the rejection under 35 U.S.C. 112, first paragraph, Applicant argues that, "in paragraph [0006], it is *at least suggested* that the problems of paragraph [0005] are overcome by the present invention, thus providing the claimed advantage at issue" (page 11 of the present response, emphasis added). Applicant further argues that the "claimed advantage" is inherent to the invention. However, Applicant provides no specific evidence that the claimed limitation is inherent. The Examiner believes that paragraphs 0005-0006 *at most* suggest or imply the claimed limitation. The Examiner notes that the cited paragraphs state that the problems of the prior art *can* be addressed by a database update and that the update may be expensive in terms of energy or bandwidth, and that the invention provides for key establishment without the difficulties

of the prior art. The Examiner believes that there is no specific solution stated in the cited paragraphs, particular not that "an update of a key distribution center database is, at least in part, capable of being avoided". At best, the avoidance of an update is only *implied* as a *possible* solution; another possible solution, for example, could be a less expensive update. However, the Examiner further notes that inherency "may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient" (*In re* Robertson, quoted at MPEP § 2163.07, cited by Applicant at page 11 of the present response).

Regarding the rejection of Claims 1, 18, and 20 under 35 U.S.C. 112, second paragraph, and specifically regarding the limitation "wherein an update of a key distribution database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar", the Examiner again notes that Applicant's remarks do not address this rejection (see also the Advisory action mailed 24 June 2005).

Regarding the rejection of Claims 2, 11, 19, and 21 under 35 U.S.C. 112, second paragraph, the Examiner first notes that the content of Claims 2, 19, and 21 has substantially been added to independent Claims 1, 18, and 20. Further, Applicant argues that, "it is purposefully not claimed at which node the operation takes place in order to provide claim breadth" (page 12 of the present response). First, however, the Examiner notes that it was, in fact, originally claimed at which node the hash value verifications take place (see, for example, originally filed claim 2). Second, the Examiner notes that the removal of specific node locations for the hash verification

raises further issues of indefiniteness under 35 U.S.C. 112, second paragraph, for Claims 8 and 11 (see below regarding these rejections). Third, the Examiner additionally notes that, in light of Applicant's specification, it is clear that one of the hash verifications takes place at the first node and the other verification at the second node, and that the locations of these verifications are vital to the functioning of the claimed protocol (see the description of Figure 6 at pages 13-16 of the present specification, in particular paragraphs 0061 and 0063).

4. All claims were rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes et al, *Handbook of Applied Cryptography*. Applicant first argues that the protocol of Menezes generally teaches that entity authentication is established as a result of nodes A and B interacting with trusted server T, but that Menezes does not disclose establishing a cryptographic key and that the trusted server T is not a suggestion of any sort of key distribution center. While the Examiner agrees that the protocol disclosed by Menezes does teach entity authentication (page 503, Protocol 12.26, "Result"), the Examiner respectfully disagrees with Applicant's further assertions. Regarding the assertion that Menezes does not disclose establishing a cryptographic key, the Examiner notes that Menezes clearly states that another result of the protocol is the establishment of a cryptographic key (page 503, Protocol 12.26, "Result"). The Examiner further notes that the chapter in which the protocol in question is disclosed is clearly entitled "Key Establishement Protocols" (see page headers for Chapter 12). Regarding the assertion that the trusted server is not a key distribution center, the Examiner notes that Menezes clearly states that the server in protocol 12.26 is a key

distribution center (see page 497, Table 12.2, where the "server type" for the Needham-Schroeder protocol, later described as Protocol 12.26, is listed as "KDC").

Further, Applicant argues that Menezes teaches using a Message Authentication Code (MAC) between parties sharing a key and not between a node and a key distribution center. This is a spurious argument, as the second node and the key distribution center, as claimed, share a key (i.e. the second node key). Applicant also argues that Menezes teaches that "the MAC *is* the shared key, but not that it is created by a key belonging to one of the parties" (page 14 of the present response). The Examiner respectfully disagrees with this characterization, noting that Menezes states that MACs are *based on* secret shared keys (see page 361, below definition 9.77) and that a MAC is created by a secret encryption key (see, for example, page 352, Section 9.5, and page 353, Algorithm 9.58).

Applicant also argues that the identity-based keying disclosed by Menezes does not suggest any sort of key being created using a node identifier and a secret key known only to the key distribution center. The Examiner respectfully disagrees, noting that Menezes discloses that an entity's identification information, along with a private key of a trusted authority (e.g. a key distribution center), are used as input to compute the entity's key (page 561, Definition 13.25).

Although Applicant argues that database updates are at least partially not required for unfamiliar participants, and states that the technique relied upon by Menezes explicitly lacks and possibly teaches away from not requiring database updates for unfamiliar participants, Applicant does not provide any evidence regarding

this argument. Applicant repeats this argument on page 17 of the present response, stating "Only applicant teaches such specific flow for the purpose of providing a technique wherein an update of a key distribution center database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Finally, Applicant suggests that there is no motivation to combine the teachings of Menezes. In response to this argument, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the motivation is as stated in the previous Office actions, namely including the use of a MAC to provide data origin authentication and data integrity (see Menezes, page 361, definition 9.77); including identity-based keying to prevent forgery and impersonation (see Menezes, page 561, section 13.4.3); and including the use of a hash, in order to provide data integrity (see Menezes, pages 321-322, section 9.1).

5. Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

Specification

6. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: independent Claims 1, 18, and 20 recite the limitation "wherein an update of a key distribution center database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar". This limitation has not been described anywhere in Applicant's specification. See below regarding the rejection under 35 U.S.C. 112, first paragraph, and see also the response to arguments above.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 1, 3-18, and 20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably

convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Specifically, independent Claims 1, 18, and 20 recite the limitation "wherein an update of a key distribution center database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar". This limitation has not been described anywhere in Applicant's specification. All other claims are rejected due to their dependence on a rejected base claim. See the response to arguments above

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 1, 3-18, and 20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 18, and 20 each recite the limitation "wherein an update of a key distribution center database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar". This limitation is generally unclear. It is not clear how something can be capable of being avoided at least in part; it would either be capable of being avoided or not. This renders the claims indefinite.

Claims 1, 18, and 20 each recite the limitation "verifying the hash value"; however, it is not clear whether the verifications take place at the first node, the second node, or the key distribution center. This renders the claims indefinite.

Claim 8 recites the limitation "validating the hash value at the second node". There is insufficient antecedent basis for this limitation in the claims.

Claim 11 recites the limitation "verifying the hash value"; however, it is not clear whether this refers to the first verification of the hash value or the second verification of the hash value recited in Claim 1.

All other claims not referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 1, 3-18, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes et al, *Handbook of Applied Cryptography*.

In reference to Claim 1, Menezes discloses the Needham-Schroeder key distribution protocol, a method that includes requesting establishing a cryptographic key between a first node and a second node, sending a message from the second node to a key distribution center that includes identifiers for the nodes (page 503, protocol 12.26, message 1), generating a cryptographic key at the key distribution center, and communicating the cryptographic key to the first and second nodes (page 503, protocol

12.26, message 2). Menezes further discloses that communicating the cryptographic key to the nodes includes encrypting the cryptographic key using the second node key to form a first encrypted key, encrypting the cryptographic key using the first node key to form a second encrypted key, sending a message from the key distribution center to the second node that includes the first and second encrypted keys (page 503, protocol 12.26, message 2), decrypting the first encrypted key at the second node to recover the cryptographic key, sending the second encrypted key and a key confirmation value to the first node (page 503, protocol 12.26, messages 3 and 5), decrypting the second encrypted key at the first node to recover the cryptographic key, establishing at the first node that the second node has the cryptographic key using the key confirmation value, and sending a message to the second node from the first node so the second node can establish that the first node has the cryptographic key (page 503, protocol 12.26, message 4).

Although the protocol does not explicitly disclose the use of message authentication codes, Menezes discloses generating and verifying MACs (see page 361, below definition 9.77; see also pages 352-359). Further, although the protocol does not explicitly disclose recreating a first node key previously created using the first node identifier and a secret key of the key distribution center or recreating a second node key previously created using the second node identifier and the secret key, Menezes further discloses identity-based keying, where an entity's key is generated using the entity's identity and a secret of a trusted server (page 561, section 13.4.3). Additionally, although the protocol does not explicitly disclose the use of a hash value in

the messages for verification, Menezes discloses that hash values can be used for verification of data (see, for example, page 322, first full paragraph). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the key distribution protocol by including the use of a MAC, in order to provide data origin authentication and data integrity (see Menezes, page 361, definition 9.77); by including identity-based keying, in order to prevent forgery and impersonation (see Menezes, page 561, section 13.4.3); and by including the use of a hash, in order to provide data integrity (see Menezes, pages 321-322, section 9.1).

In reference to Claims 3 and 4, Menezes further discloses that the messages include the node identifiers and a nonce (page 503, protocol 12.26, message 1).

In reference to Claim 5, Menezes further discloses verifying the message authentication code by creating a test MAC to compare with the original MAC (pages 321-322, section 9.1).

In reference to Claim 6, 8, and 11, Menezes further discloses verifying the hash value by creating a hash value and creating test hash values to compare with the original hash value (page 322, first full paragraph).

In reference to Claim 7, Menezes further discloses that a message includes the node identifiers and the encrypted keys (page 503, protocol 12.26, message 2).

In reference to Claims 9 and 10, Menezes further discloses that a message includes identifiers, a nonce, and a confirmation value that includes an encrypted nonce (page 503, protocol 12.26, message 5).

In reference to Claims 12 and 15, Menezes discloses that each node confirms that the other has the cryptographic key by verifying nonces (page 503, protocol 12.26, messages 4 and 5).

In reference to Claims 13 and 14, Menezes further discloses that a message includes identifiers and an encrypted confirmation value (page 503, protocol 12.26, message 4).

In reference to Claims 16 and 17, Menezes discloses identity-based keying (page 561, section 13.4.3) and that the node keys are installed in the node prior to deployment (page 503, protocol 12.26, "One-time setup").

Claim 18 is directed to software implementations of the method of Claim 1, and is rejected by a similar rationale.

Similarly, Claim 20 is directed to an apparatus corresponding substantially to the method of Claim 1, and is rejected by a similar rationale.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137